Implications of SDN Denial of Service Mitigation

John C. Hoag, Bahast Saber, Ohio University {hoagj, sb705112} @ ohio.edu

Workshop on Science of Security through Software-Defined Networking

SoSSDN

Abstract

This work continues research on “State Based Network Management” which developed a broad CONOPS for an SDN-like CoS-aware controller for provisioning network elements.

This work resides in an endowed telecom academic program with extensive virtualization capabilities, awareness of E2E performance, and capabilities in open source.

Institutional Motivations:

- Become fluent in implementing, testing, and visualizing ACL Rules in Southbound context.
- Pursue automation of Southbound use case in “brownout” scenario, forcing reprovisioning.
- Pursue automation of Southbound use case in multipoint scenario.
- Enhance scope to include FW, IDS/IPS functions.
- Further deploy in virtualized East-West use case between virtual servers and SAN (in lab).
- Contribute to companion activities, scope to include Northbound load balancing, etc.

SDN Testbed for DDoS

Current instructional environment is simulation-only.

Proposed environment utilizes simulation tool Mininet to create topology, then implement controller separately.

Initial project outcome is to determine preference between Floodlight and Open Daylight based on meeting anticipated requirements and on performance in testing.

Virtualized testbed includes traffic source and sink desktops as well as controller and console host and switch. Respective consoles utilize Java and Python, via Eclipse, to modify Southbound ACL Rules for Floodlight and ODL, respectively.

Traffic sources include iperf (TCP and UDP) as well as nmap and ping; traffic capture via Wireshark, with Hyperglance providing an overview. The definitive DDoS tools are HOIC and LOIC - which may be utilized. SNMP may be used later for stress testing related to depth of rule sets.

SoSSDN Research Questions

Q1. What is the real performance envelope for virtualizing security functions, i.e., where are the hard limits and how are they expressed, as well as the knees or inflection points? What is the real tradespace for security and performance under virtualization?

Q2. What are the taxonomy and ontology for discussing virtualized security functions, absent appliance hardware? What are the main branches?

Q3. At what point are feature interactions a concern, either in terms of functionality or performance?

Q4. What, if any, are the latent vulnerability issues in regard to virtual security, especially when comparing open source and commercial products?

Q5. Are we underestimating the use cases for virtual security – especially with respect to 5G and SD-WAN, and avoidance of MPLS and commercial “traffic trombones”?

Methodology & Expected Results

Project has very observable results: packets are permitted or denied based on rule state; rule transmission is easily captured and parsed.

Discipline is needed to create unit test cases for more advanced scenarios. Sandbox nature of testbed permits exercising policy enforcement under various load levels.

References

State-Based Network Management: Semantic Reasoning for Adaptive Management of Telecommunications Networks, John C. Hoag; Frederick A. Hayes-Roth, 2006 IEEE International Conference on Systems, Man and Cybernetics.

An Architecture for Network Operations and Management Based on State and Services, J. C. Hoag, 2006 1st IEEE International Workshop on Broadband Convergence Networks.

State-based Network Management: From The Electricity Grid to The Global Information Grid, J. C. Hoag; C. Gunderson, MILCOM 2005 - 2005 IEEE Military Communications Conference.

INFORMATION TRUST INSTITUTE

ILLINOIS

SCIENCE OF SECURITY VIRTUAL ORGANIZATION